**IN THE DRAWINGS**

With the consent of the Examiner, applicants propose to amend Figure 4 of the drawings in accordance with the red ink notations on the accompanying copy of Figure 4. New formal drawings are being submitted contemporaneously herewith.

**REMARKS**

On page 2 of the Office Action, the Examiner required correction of a typographical error. Accordingly, the claims have been amended to correct this error.

On pages 2 and 3 of the Office Action, the Examiner rejected claims 1, 2, 7, 13, and 14 under 35 U.S.C §102(e) as being anticipated by Berardi.

Berardi illustrates in Figure 1A an RFID transaction system 100A whose operation begins when a fob 102 is presented for payment, and is interrogated by an RFID reader 104 or, alternatively, by an interface 134. The fob 102 and the RFID reader 104 then engage in mutual authentication after which the fob 102 provides a transponder identification and/or account identifier to the RFID reader 104 which in turn provides this information to a POS device 110 of a merchant system 130.

The fob 102 has a transponder 114 for providing RF communication with the reader 104. Instead of a fob 102, any device having a transponder, such as a key ring, tag, card, cell phone, or wristwatch, can be used to communicate with the RFID reader 104 via RF communication.

The RFID reader 104 has an RFID internal antenna 106. Alternatively, the RFID reader 104 may include an external antenna 108 for communications with the fob 102. The RFID reader 104 communicates with the merchant system 130 via a data link 122. The user interface 134 is connected to a network 136 and to the transponder via a USB connector 132. The POS device 110 is in further communication with a customer interface 118 (via a data link 128) for entering at least customer identity verification information. In addition, the POS device 110 may be in communication with a merchant host network 112 (via a data link 124) for processing any transaction request.

Figure 2 of Berardi is a block diagram of the fob 102. The fob 102 includes an antenna 202, a modulator and demodulator 206, a protocol/sequence controller 208, and authentication circuitry 210 that facilitates authentication of the signal provided by the RFID reader 104, and a secure memory database 212.

The protocol/sequence controller 208 is in communication with a database 214 for storing account data and an unique identification code associated with the fob 102. The data stored in the database 214 may be unencrypted.

The RFID reader 104 may provide more than one RF interrogation signal. In this case, the fob 102 would include one or more additional RF signal receiving and transmitting units 226. The fob 102 may further include a universal serial bus (USB) connector 132 for interfacing the fob 102 to the user interface 134. The user interface 134 is in communication with the POS device 110 via a network 136 such as the Internet, an intranet, or the like. No RFID reader is required in this case since the connection to POS device 110 may be made using the USB port on user interface 134 and the network 136.

As shown in Figure 9, the fob 102 may include a biometric security system 902 having a biometric sensor 904 for sensing the fingerprint of the user of the fob 102. A sensor interface/driver 906 receives the sensor fingerprint and activates the operation of the fob 102. Thus, the user places his finger on the biometric sensor 904 to initiate operation of the fob 102, or to provide secondary verification of the user's identity. The sensor fingerprint may be digitized and compared against a digitized fingerprint stored in the secure database 212 included on fob 102.

The biometric security system 902 may be used to authorize a purchase exceeding the established per purchase spending limit. Thus, when the customer's intended purchase exceeds the spending limit, the customer may be asked to provide assurance that the purchase is authorized. Accordingly, the customer may provide such verification by placing his finger over the biometric sensor 904. The biometric sensor 904 may then digitize the fingerprint and provide the digitized fingerprint for verification as described above (i.e., the fob 202 compares the digitized fingerprint with data stored in the memory 212 of the fob 202). Once verified, the fob 102 then provides a transaction authorized signal to the RF transponder 202 or to the transponder 220 for forwarding to the RFID reader 104.

Figure 3 is a block diagram of the RFID reader 104. The RFID reader 104 includes the antennas 106 and 108 coupled to a RF module 302, which is further coupled to a control module 304. The RF module 302 and the antenna 106 facilitate communication with the fob 102. The reader 104 has a secure database 310 which stores data corresponding to the fobs 102 that are authorized to transact business over the system 100.

Figure 4 is a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process is depicted as one-sided. That is, the flowchart depicts the process of the RFID reader 104 authenticating the fob 102, although similar steps may be followed in the instance that fob 102 authenticates RFID reader 104.

Independent claim 1 is directed to a security system reader comprising a transceiver and a processor. The transceiver transmits a stimulus signal and receives a signal containing an authentication code. The processor determines whether the received authentication code is from a badge or a fingerprint keyfob, and performs an authentication of the authentication code dependent upon whether the authentication code is from the badge or from the fingerprint keyfob.

Berardi fails to disclose this apparatus.

The Examiner interprets the fob shown in Figure 2 of Berardi as the badge of independent claim 1 and the fob shown in Figure 9 of Berardi as the keyfob of independent claim 1. However, the processing that is performed by the reader 104 is not dependent upon whether the authentication code is from the fob of Figure 2 or the fob of Figure 9.

Indeed, the processing that is performed by the reader 104 is the same whether the signal comes from the fob of Figure 2 or the fob of Figure 9. That this is so can be seen by considering that the fingerprint taken by the sensor 904 of the fob of Figure 9 is not sent to the reader but is only used internally by the fob to permit only an authentic user to use the fob. This use of the fingerprint is disclosed in paragraphs 0063-0066, 0140, and 0141 of Berardi.

Therefore, since the reader does not receive the fingerprint, the processing of the reader is not dependent upon whether the authentication code is from the badge or from the fingerprint keyfob.

For this reason, independent claim 1 is not anticipated by Berardi.

Independent claim 7 is directed to a method of providing access comprising receiving a signal containing an authentication code, determining whether the authentication code is from a badge or a fingerprint keyfob, determining whether the authentication code is authentic dependent upon whether the authentication code is from the badge or from the fingerprint keyfob, and, if the authentication code is authentic, permitting access.

As discussed above, Berardi fails to disclose processing that is dependent upon whether a received authentication code is from a badge or from a fingerprint keyfob as required by independent claim 7.

Therefore, independent claim 7 is not anticipated by Berardi.

Independent claim 14 is directed to a method of providing access comprising receiving a signal containing an authentication code, determining whether the authentication code is from a badge or a keyfob, determining whether the authentication code is authentic, and, if the authentication code is authentic, permitting access.

As discussed above, the reader of Berardi cannot determine whether an authentication code is received from a badge or a keyfob as required by independent claim 14 because there is no disclosure in Berardi that the code received from the fob of Figure 2 is different from the code received from the fob of Figure 9. Indeed, as discussed above, there is no disclosure in Berardi that the fingerprint is sent to the reader.

Therefore, independent claim 14 is not anticipated by Berardi.

Because independent claims 1 and 7 are not anticipated by Berardi, dependent claims 2 and 13 are likewise not anticipated by Berardi.

In addition, dependent claim 2 recites that the authentication code received from the fingerprint keyfob comprises a fingerprint signature. As discussed above, the reader disclosed in Berardi does not receive a fingerprint because the fingerprint is used only internally by the fob.

Therefore, for this reason also, dependent claim 2 is not anticipated by Berardi.

On pages 3 and 4 of the Office Action, the Examiner rejected claims 4, 5, 8, 10, 11, 15, 16, 18, 20, 22, and 23 under 35 U.S.C §103(a) as being unpatentable over Berardi in view of Fuku.

Fuku discloses in Figure 1 an authentication unit 1 having a fingerprint sensor 11, a feature extracting unit 12, a feature storage unit 13, a fingerprint verification unit 14, and a control unit 15. The fingerprint sensor 11 capture a fingerprint image of a user's finger. The feature extracting unit 12 extracts fingerprint information from the fingerprint image captured by the fingerprint sensor 11. The feature storage unit 13 stores reference fingerprint information

about fingerprints of authorized users. The fingerprint verification unit 14 verifies the identity of the user by comparing the fingerprint information extracted by the feature extracting unit 12 against the reference fingerprint information stored in the feature storage unit 13. The control unit 15 switches between a plurality of processing modes according to signals from a brake pedal sensor 4 and an accelerator pedal sensor 5. The control unit 15 also controls a door lock driving unit 2 and an engine control unit 3 according to a verification result from a key ID acquiring unit 6 for verifying the identity of a mechanical key 7 and according to the verification result from the fingerprint verification unit 14.

The door lock driving unit 2 locks or releases doors according to a control signal from the control unit 15. The engine control unit 3 allows or prohibits users to start the engine according to a control signal from the control unit 15. The key ID assigned to the mechanical key 7 is used by the key ID acquiring unit 6 to determine whether or not the key 7 is an authorized key.

In Figure 3, Fuku shows an embodiment in which a navigation unit 21 having an operation unit 26, such as

a switch, replaces the brake pedal sensor 4 and the accelerator pedal sensor 5 of Figure 1. In Figure 4, Fuku shows an embodiment in which a connector 31 and a failure diagnosis unit 41 replaces the brake pedal sensor 4 and the accelerator pedal sensor 5 of Figure 1. The operation unit 26 of the navigation unit 21 shown in Figure 4 and the failure diagnosis unit 41 correspondingly cause switching between the various processing modes.

As can be seen, Fuku does not disclose or suggest a reader that is capable of operating with either a badge or a keyfob as required by independent claims 1, 7, and 14. Accordingly, because Berardi also does not disclose or suggest a reader that is capable of operating with either a badge or a keyfob as required by independent claims 1, 7, and 14, the combination of Berardi and Fuku would not have suggested the inventions of independent claims 1, 7, and 14 to one of ordinary skill in the art.

Therefore, independent claims 1, 7, and 14 are patentable over Berardi in view of Fuku. Because independent claims 1, 7, and 14 are patentable over Berardi in view of Fuku, dependent claims 4, 5, 8, 10,

11, 15, 16, 18, 20, 22, and 23 are likewise patentable over Berardi in view of Fuku.

On pages 4 and 5 of the Office Action, the Examiner rejected claims 3, 6, 9, 12, 17, 19, 21, and 24 under 35 U.S.C §103(a) as being unpatentable over Berardi in view of Fuku and further in view of Fitzgibbon.

Fitzgibbon shows in Figure 2 a hand-held transmitter that has an input in the form of a fingerprint device and an output in the form of an antenna radiating radio frequency information. Fingerprint data information from the fingerprint device are sent to a control circuit that outputs data to a radio frequency circuit coupled to the antenna.

The fingerprint device includes a window against which a user's thumb is pressed. The fingerprint provides a biometric identification unique to the user's anatomy. The sensed fingerprint is compared against reference fingerprints stored in a non-volatile memory. The control circuit performs only simple line level and pulse squaring functions on the incoming data from the fingerprint device. The output of the control circuit is in digital pulse form and is fed to the RF circuit.

The information passed through the RF circuit and radiated by the antenna is of a trinary rolling code

data type having both rolling code and fixed code digits. The control circuit combines this information with a device code indicating the type of transmitter. The device code can also include a serial number.

Figure 3 shows a wall mounted transmitter having the same schematic form as the hand-held transmitter system, but includes a device code different from that of other types of hand-held and other transmitter devices.

Figure 4 shows a receiver/barrier operator that controls a motor to open or close a movable barrier such as a gate or a garage door. A receiving antenna directs RF information to an RF receiver which passes the receive information to a control circuit. The received information is in the form of both a rolling code and a fixed code. The control circuit confirms if the received signal is authorized with respect to the rolling code. The control circuit processes the fingerprint data. The control circuit includes non-volatile memory, which stores previously acquired fingerprint data corresponding to different authorized users. If a match is found, and optionally if rolling code authentication is proven, then the motor opens or closes the garage door.

Operation of either the transmitter 100 or 120 is shown in Figure 5. When the transmitter is energized, the fingerprint window is continuously scanned to detect if the user's thumb is pressed against the device. Once a finger press is detected, the fingerprint data is combined with the rolling code data. The combined data is transmitted as a radio frequency signal.

As can be seen, Fitzgibbon does not disclose or suggest a reader that is capable of operating with either a badge or a keyfob as required by independent claims 1, 7, and 14. Accordingly, because Berardi and Fuku also do not disclose or suggest a reader that is capable of operating with either a badge or a keyfob as required by independent claims 1, 7, and 14, the combination of Berardi, Fuku, and Fitzgibbon would not have suggested the inventions of independent claims 1, 7, and 14 to one of ordinary skill in the art.

Therefore, independent claims 1, 7, and 14 are patentable over Berardi in view of Fuku and further in view of Fitzgibbon. Because independent claims 1, 7, and 14 are patentable over Berardi in view of Fuku and further in view of Fitzgibbon, dependent claims 3, 6, 9, 12, 17, 19, 21, and 24 are likewise patentable over

Berardi in view of Fuku and further in view of Fitzgibbon.

New added independent claim 26 is directed to a method of providing access comprising receiving a signal containing an authentication code, determining whether the authentication code is of a first type or of a second different type, processing the authentication code in a first manner if the authentication code is of the first type and processing the authentication code in a second different manner if the authentication code is of the second different type to determine whether the authentication code is authentic, and, if the authentication code is authentic, permitting access.

Berardi, Fuku, and/or Fitzgibbon do not disclose or suggest a reader that is capable of authenticating codes of different types as required by independent claim 26. Accordingly, Berardi, Fuku, and/or Fitzgibbon would not have suggested the invention of independent claim 26 to one of ordinary skill in the art.

Therefore, independent claim 26 and the claims dependent thereon are patentable over Berardi, Fuku, and/or Fitzgibbon.

## CONCLUSION

In view of the above, the claims of the present application patentably distinguish over the art applied by the Examiner. Accordingly, allowance of these claims and issuance of the present application are respectfully requested.

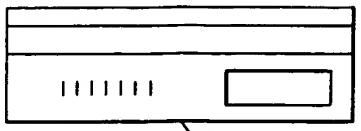
Respectfully submitted,

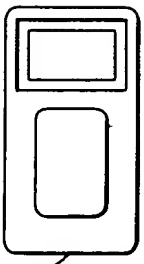
Schiff Hardin LLP
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
(312) 258-5500
Customer No. 000128

By: _____
Trevor B. Joike
Reg. No: 25,542

July 25, 2006

# FIG. 4




TRANSMIT RF AUTHENTICATION ID CONTAINING KEYCARD IDENTIFIER TOKEN

TRANSMIT RF AUTHENTICATION ID WITH FINGERPRINT KEYFOB IDENTIFIER TOKEN, FINGERPRINT DIGITAL IMAGE, AND ROLLING KEYFOB CODE.

60

READ RF AUTHENTICATION ID — 62

64

IS AUTHENTICATION ID FROM HIGH SECURITY KEYFOB?

NO

YES

AUTHENTICATE BADGE FROM LIST OF AUTHORIZED IDs. — 66

USE ENHANCED FINGERPRINT AUTHENTICATION ALGORITHM WITH HIGH ENCRYPTION AND ROLLING CODE TO IDENTIFY AUTHORIZED PERSON. — 74

68

IS THE PERSON AUTHORIZED?

72

NO

YES

70

DENY ENTRY, SINGLE ALARM.

GRANT ENTRY, OPEN DOOR.